
超ドラフト版

- Interdomain Routing Security Workshop -
ISP のルータにおいて設定を推奨するフィルタの項目について

馬渡 将隆 [MAWATARI Masataka]
Dream Train Internet, Inc.
2005/01/13

1. 目的の概要

インターネットの安定性を保つ為に、ISP の内部および外部の接続部分において、ISP で運用をしているルータに設定をする事が推奨されるフィルタをまとめた文書です。

下記の 3. の部分に記載してありますが、"最低限、設定をする事が推奨されるフィルタ" については、ISP 相互での運用部分において基本的な部分となるので、文字通り最低限設定をする必要があると考えます。

この文書では、以下の項目を前提とした元にフィルタを考えてまとめてあります。

- o エンドユーザの通信には影響しない事
- o 不必要な経路は出さない/受け取らない事
- o 不必要なパケットは出さない/受け取らない

2. 言葉の定義

1. この文書に表記してある "Prefix フィルタ" とは、"Prefix Based フィルタ" の事を指します。
2. この文書に表記してある "経路フィルタ" とは、"Prefix Based フィルタ" および "AS-PATH フィルタ" の双方を包括したフィルタの事を指します。
3. この文書に表記してある "トランジット" とは "フルルートの広告を受けている接続点" もしくは "フルルートの広告を受けている状態" の事を指します。

3. この資料のまとめ方

以下の項目のとおりフィルタのまとめてあります。

1. 最低限設定をする事が推奨されるフィルタ
 - 1.1 AS 内部でのパケットフィルタ
 - 1.2 ピアおよびトランジットに対するパケットフィルタ
 - 1.3 ピアおよびトランジットに対する経路フィルタ
 - 1.4 IX セグメントに対する経路フィルタ
2. リソース (運用者、ルータ) により設定をする事が推奨されるフィルタ
 - 2.1 AS 内部でのパケットフィルタ
 - 2.2 ピアおよびトランジットに対するパケットフィルタ
 - 2.3 ピアおよびトランジットに対する経路フィルタ

3. フィルタの運用を軽減する為に有効な技術について

4. 目次

1. 最低限設定をする事が推奨されるフィルタ

1.1 AS 内部でのパケットフィルタ

- 顧客接続ルータでの Ingress Source アドレスパケットフィルタ
 - Special-Use IP アドレスを reject するパケットフィルタ (プライベートアドレス、Host Loopback、Multicast など)
- 顧客接続ルータでの Egress Source アドレスパケットフィルタ
 - Special-Use IP アドレスを reject するパケットフィルタ (プライベートアドレス、Host Loopback、Multicast など)
- ルータ自体のアクセスに対するパケットフィルタ
 - telnet, snmp, syslog などルータで動かしているサービスについてのフィルタ

1.2 AS 間 (ピアおよびトランジットに対するフィルタ) でのパケットフィルタ

- BGP ルータでの BGP (179/TCP) Ingress パケットフィルタ
 - 自 AS 内、IX セグメント、プライベートピアのセグメントからのみの BGP パケットを accept するパケットフィルタ

1.3 AS 間 (ピアおよびトランジットに対するフィルタ) での経路フィルタ

- ピアおよびトランジットに対する Ingress Prefix フィルタ
 - Special-Use IP アドレスを reject する Prefix フィルタ (プライベートアドレス、Host Loopback、Multicast など)
- ピアおよびトランジットに対する Egress Prefix フィルタ
 - Special-Use IP アドレスを reject する Prefix フィルタ (プライベートアドレス、Host Loopback、Multicast など)
- 自 AS が持っている Prefix の or longer を reject する Ingress Prefix フィルタ

1.4 IX セグメントに対する経路フィルタ

- 自 AS が接続をしている IX のセグメントの or longer を reject する Ingress Prefix フィルタ

2. リソース (運用者、ルータ) のリソースにより設定をする事が推奨されるフィルタ

2.1 AS 内部でのパケットフィルタ

- 顧客接続ルータでの Ingress Source アドレスパケットフィルタ
 - 顧客に割り当てたアドレスのみを accept するパケットフィルタ

2.2 ピアおよびトランジットに対するパケットフィルタ

- ピアから受け取る Prefix の Ingress Prefix フィルタ
 - ピア接続をしている ISP からの更新通知を元にフィルタの運用をする
- 細かい経路を reject する Ingress Prefix フィルタ

- Un-Allocated (未割り当て) Ingress Prefix フィルタ
 - Bogon List を参照してフィルタの運用をする
- RIR's Minimum Allocation Size の Ingress Prefix フィルタ

3. フィルタの運用を軽減する為に有効なその他の技術について

3.1 Max-Prefix Limits

- 異常な経路数を受け取らないようにする為

3.2 TTL-Sanity-Check

- 設定をした TTL 値の範囲外のパケットが来た場合に、そのパケットを reject する

3.3 uRPF

- 経路情報を利用してフィルタをする
